

Troubleshooting de Falha de Transferência de Arquivo SPOG PCCE 12.0

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solução](#)

Introduction

Este documento descreve como solucionar problemas de falha na transferência de arquivos do Cisco Packaged Contact Center Enterprise (PCCE) 12.0 Single Pane Of Glass (SPOG).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- PCCE
- Porta de voz do cliente (CVP)

Componentes Utilizados

As informações neste documento são baseadas no PCCE 12.0.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problema

No PCCE SPOG, para transferência de arquivos, navegue para **SPOG > OverView > Call Settings > IVR Settings > File Transfers**. Às vezes, a transferência falha conforme mostrado na imagem:



| Job ID | State | Creation Time | Description |
|-------------------------------|---|---------------|-------------|
| <input type="checkbox"/> 5004 | ● Failed | | |

Solução

1. Navegue até **Job** e selecione **Log File** como mostrado na imagem.

IVR Settings

View Job ID 5004

State ● Failed

Description

Host



Creation Time



Start Time



Total Time

0 min, 6 sec

Job Details



Log File

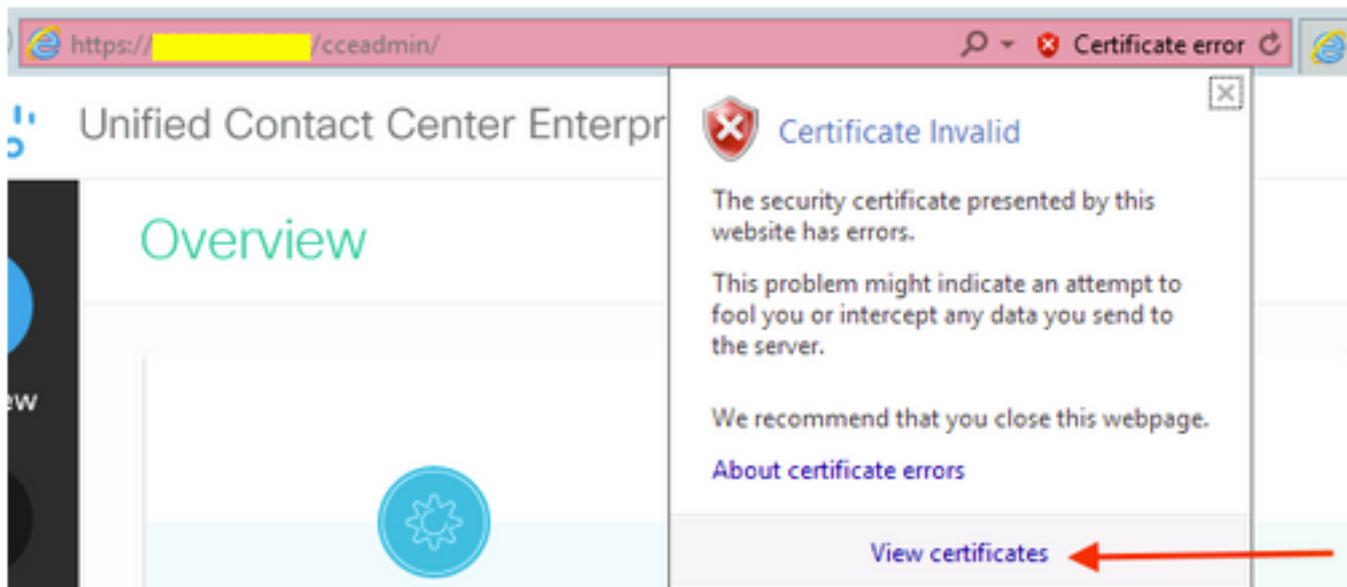


Aviso para a mensagem de erro

```
"Deployment of https://<FQDN of AW node>:443/unifiedconfig/config/downloadablefiles/ivrapplication/<FileName>.zip completed on <CVP FQDN> with status as sun.security.validator.ValidatorException: No trusted certificate found."
```

Este erro indica que há um problema aqui devido ao certificado AW não ser confiável pelo CVP. As etapas que podem corrigir essa situação são:

2. Copie o arquivo de certificado do URL do SPOG, como mostrado na imagem.



3. Copie este arquivo de certificado para o nó CVP onde o arquivo ZIP original precisa ser transferido para um diretório:

```
C:\cisco\cvp\conf\security
```

4. Em seguida, copie a senha do armazenamento de chaves do local:

```
keystore password from : %CVP_HOME%\conf\ and open the security.properties
```

5. Da mesma forma, para onde foi copiado o certificado AW; abra o Command Prompt como Administrador e execute o comando:

```
cd %CVP_HOME%\jre\bin
```

6. Use este comando para importar os certificados AW para o servidor CVP.

```
keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\keystore -storetype JCEKS -alias  
<FQDN of AW Node> -file C:\Cisco\CVP\conf\security\<Name of the AW SPOG certificate>.cer
```

7. No prompt de senha, cole a senha copiada do **security.properties**.

8. Digite **Yes** para confiar no certificado e garantir que você obtenha o resultado de que Certificate foi adicionado ao keystore.

Há um aviso avisado junto com a importação bem-sucedida. Isso é devido ao formato proprietário Keystore e pode ser ignorado.

9. Reinicie o serviço cvpcallserver, vxmlserver e wsm em nós CVP.